PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-323351
(43)Date of publication of application : 14.11.2003

(51)Int.Cl. G06F 12/14
G11B 20/10
G11B 20/12
G11B 27/00
H04L 9/08
H04L 9/32

(21)Application number : 2003-050043 (71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(22)Date of filing : 26.02.2003 (72)Inventor : MIYAMOTO HARUTOSHI

(30)Priority
Priority number : 2002050963 Priority date : 27.02.2002 Priority country : JP

(54) COPYRIGHT MANAGEMENT SYSTEMCOPYRIGHT MANAGEMENT METHODHOST DEVICEPROGRAM AND RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a copyright protection system and a copyright protection method that are easy for users to usea host device therefora program therefor and a recording medium carrying the program.
SOLUTION: The host device encrypts prescribed contents by a prescribed encryption methodselects a specific reproducer 5 in dependence on the number of reproducers 5 preauthorized for reproductionand sends decryption information such as a decryption key for decrypting the encrypted contents 6 to the selected specific reproducer 5.

CLAIMS

[Claim(s)]
[Claim 1]A host device which sends decoding information for choosing specific playback equipment and decrypting said enciphered contents to said specific selected

playback equipment according to the number of playback equipment to which reproduction was permitted while enciphering predetermined contents with a predetermined encryption method.
[Claim 2]The host device according to claim 1 further provided with a selection indication means for directing said selection.
[Claim 3]The host device according to claim 1 with which said encryption uses host ID peculiar to said host deviceand apparatus ID and said host ID of said specific playback equipment are contained in said decoding information.
[Claim 4]The host device according to claim 1 which said predetermined contents and information on said number are enciphered from a distributing serverand is distributed.
[Claim 5]Apparatus ID which host ID which contents enciphered by a host device haveand host ID contained in said decoding information are in agreementand is contained in said decoding informationOn condition that peculiar apparatus ID is in agreementare said enciphered contents playback equipment to reproduceand said host deviceWhile enciphering predetermined contents using peculiar host IDPlayback equipment which chooses specific playback equipment and sends decoding information in which apparatus ID and said host ID of said specific playback equipment for decrypting said enciphered contents to said specific selected playback equipment are contained according to the number of playback equipment to which reproduction was permitted.
[Claim 6]The playback equipment according to claim 5 by which said playback equipment is not connected to the Internet.
[Claim 7]A distributing server which distributes predetermined contentsand a host device which enciphers predetermined contents with a predetermined encryption methodHave playback equipment which reproduces said enciphered contentsand said host deviceSaid specific playback equipment is chosen according to the number of playback equipment to which reproduction was permittedA copyright management system which sends decoding information for decrypting said enciphered contents to said specific selected playback equipment and by which said playback equipment reproduces said enciphered contents using said sent decoding information.
[Claim 8]A distributing server which distributes predetermined contentsand a host device which enciphers said predetermined contents with a predetermined encryption methodAre a copyright management system provided with playback equipment which reproduces said enciphered contents the used copyright management methodand said host deviceSaid specific playback equipment is chosen according to the number of said playback equipment to which reproduction was permittedA copyright management method that send decoding information for decrypting said enciphered contents to said specific selected playback equipmentand said playback equipment reproduces said enciphered contents using said sent decoding information.
[Claim 9]A program for operating a host device which enciphers predetermined contents of the copyright management system according to claim 7 with a

predetermined encryption methodand playback equipment which reproduces said enciphered contents as a computer.
[Claim 10]It is the recording medium which made the program according to claim 9 supportand is an available recording medium with a computer.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention relates to the copyright management system and the copyright management method of performing license management of the copyright of contentsits host deviceits programand the recording medium of the program.
[0002]
[Description of the Prior Art]In recent yearsthe music form reproduced from the sound source of origin not only like CD-DA but mp3 (mpeg audio layer3) is widely used for the user. Howeversince the method of copyright management is not established to mp3it has been a big problem for an owner of a copyrightand the means which is going to solve this is proposed. The method of copyright management is examined also about digital contentssuch as not only music but an imageand a picture. For examplethe system called DRM (Digital Right Management) in the copyright management of music compression technology called WMA (Windows (registered trademark) Media Audio) used on a personal computer is adopted. This is a system with which peculiar ID of the enciphered equipment is needed for a decoding of the enciphered music.
Spread of an illegal copy can be prevented by limiting an enciphering device and playback equipment to the same equipment.
The system which protects the copyright of delivery information is proposed also in the information distribution system which targeted sized terminalssuch as a cellular phone (for examplerefer to patent documents 1). The information distributed from the distributing server and peculiar ID of the cellular phone of a distribution destination are registered into the management data base on a serverand it has become the structure which can reproduce information only with the registered cellular phone.
[0003]
[Patent documents 1] JP2001-78266A[0004]
[Problem to be solved by the invention]Howeversince it will be the requisite that each equipment can access the server on a networkit is not realizable with the playback equipment on condition of network connectionetc.
[0005]Ways the playback equipment which cannot access a network directly performs license management of copyright include the method shown in drawing 13. In drawing

13101 is an electronic music distribution (EMD) server.
The media in which 102 has an Internet line103 has users' personal computerand 104 has peculiar IDfor examplean SD card(Secure Digital card)and 105 are the general-purpose playback apparatus 105 which is not connected to the Internet line.

[0006]Herecheck-in is transmitted and receivedand data is transmitted between the personal computer 103 and SD card 104 and received by a check-out system. While check-in of data and check-out manage the number of times of a copy of datait says transmitting and receiving data between a personal computerand an external instrument and media. Check-out means transmitting data to an external instrument and media from a personal computer. In this casewhen data has restricted frequency of check-out (copy)the check-out exceeding restricted frequency cannot be performed. Check-in means returning an external instrument and the data transmitted to media to the personal computer of the source from a personal computerso that it may not remain in those external instruments and media. The data in which he was checked out in this case can be returned only to the personal computer of the source. Howeverhe can check out again the data returned to the personal computer by check-in.
[0007]According to this methodby treating contents together with peculiar ID of SD card 104 which is mediathe original copy and duplicate of contents are distinguished and copyright management is performed. The illegal copy of data is prevented by specifically checking out the data of contents only to attested SD card 104. That isa user downloads contents data with users' personal computer 103 via Internet line 102 from EMD server 101. By inserting SD card 104 in the personal computer 103the personal computer 103 checks that predetermined ID with which SD card 104 is attested beforehand is given. The personal computer 103 checks out contents data from the personal computer 103 next. And if SD card 104 in which desired contents data was incorporated is inserted in the general-purpose playback apparatus 105the general-purpose playback apparatus 105 can reproduce desired contents by things.
[0008]Howeverthe duplicate more than a predetermined number is impossible for desired contents data by check-out of the personal computer 103and the function of tic yne. The contents of the above-mentioned request Thereforea portable playera minicomponentWhen it is going to reproduce with two or more general-purpose playback apparatus 105such as a car stereothere is inconvenience that SD card 104 in which contents data is recorded must be carriedand SD card 104 must be set to the general-purpose playback apparatus 105 each time. In the above-mentioned methodas for performing two or more reproductionseven if it is less than a predetermined number since SD card 104 is comparatively expensiveexpense starts so muchand there is a fault of being hard to spread through a user.
[0009]Thusin the above copyright management systemsit was hospitable to a contents distribution contractor's protectionand there was the side in which the

user's user-friendliness had fallen victim.
[0010]How to use MD107 which is general-purpose media is shown in drawing 14 instead of using SD card 104. In the system shown in drawing 14a different point from the system shown in drawing 13 is a point of MD107 passing ID appendix sound apparatus 106and being checked in and checked out by the personal computer 103. Namelyin order to incorporate desired contents data into MD107. After checking that ID with which the personal computer 103 attests ID appendix sound apparatus 106and ID appendix sound apparatus 106 is attested beforehand is givendesired contents data is checked out by MD107 via ID appendix sound apparatus 106 from the personal computer 103.
[0011]Since cheap MD107 can be used according to such a systemcompared with a case where performing two or more reproductions reproduces using SD card 104expense is cheap and ends. Howeverfor every transmission and reception of datasince proceduresuch as attestation and cipher processingwas requireda highly efficient processing circuit was needed at check-in of ID appendix sound apparatus 106 to the personal computer 103and check-out for ID appendix sound apparatus 106. Load of attestation and cipher processing is large and it is not easy to use a user.
[0012]The purpose of this invention aims at providing a user-friendly copyright protection system for a usera copyright protection methodits host deviceits programand a medium that supported the program in consideration of above-mentioned SUBJECT.
[0013]
[Means for solving problem]The 1st this invention for solving an aforementioned problemWhile enciphering predetermined contents with a predetermined encryption methodaccording to the number of playback equipment (5) to which reproduction was permittedIt is a host device which sends decoding information (7) for choosing specific playback equipment (5) and decrypting said enciphered contents (6) to said specific selected playback equipment (5).
[0014]The 2nd this invention is the host device according to claim 1 further provided with a selection indication means for directing said selection.
[0015]The 3rd this invention is a host device of the 1st this invention with which said encryption uses host ID peculiar to said host deviceand apparatus ID and said host ID of said specific playback equipment (5) are contained in said decoding information (7).
[0016]The 4th this invention is a host device of the 1st this invention which said predetermined contents and information on said number (38) are enciphered from a distributing server (1)and is distributed.
[0017]Host ID which contents (6) as which the 5th this invention was enciphered by a host device haveApparatus ID which host ID contained in said decoding information (7) is in agreementand is contained in said decoding information (7)On condition that peculiar apparatus ID is in agreementare said enciphered contents (6) playback equipment to reproduceand said host deviceWhile enciphering predetermined contents

using peculiar host IDSpecific playback equipment (5) is chosen according to the number of playback equipment (5) to which reproduction was permittedIt is playback equipment which sends decoding information (7) in which apparatus ID and said host ID of said specific playback equipment (5) for decrypting said enciphered contents (6) are contained to said specific selected playback equipment (5).

[0018]The 6th this invention is playback equipment of the 5th this invention by which said playback equipment (5) is not connected to the Internet.

[0019]A distributing server (1) with which the 7th this invention distributes predetermined contentsHave a host device (3) which enciphers predetermined contents with a predetermined encryption methodand playback equipment (5) which reproduces said enciphered contentsand said host device (3)Said specific playback equipment (5) is chosen according to the number of playback equipment (5) to which reproduction was permittedSending decoding information (7) for decrypting said enciphered contents (6) to said specific selected playback equipment (5)said playback equipment (5) is a copyright management system which reproduces said enciphered contents (6) using said sent decoding information (7).

[0020]A distributing server (1) with which the 8th this invention distributes predetermined contentsA host device (3) which enciphers said predetermined contents (1) with a predetermined encryption methodAre a copyright management system provided with playback equipment (5) which reproduces said enciphered contents the used copyright management methodand said host device (3)Said specific playback equipment (5) is chosen according to the number of said playback equipment (5) to which reproduction was permittedSending decoding information for decrypting said enciphered contents (6) to said specific selected playback equipment (5)said playback equipment (5) is the copyright management method which reproduces said enciphered contents (6) using said sent decoding information (7).

[0021]The 9th this invention is a program for operating the host device (3) which enciphers the predetermined contents of the copyright management system of the 7th this invention with a predetermined encryption methodand the playback equipment (5) which reproduces said enciphered contents (6) as a computer.

[0022]The 10th this invention is the recording medium which made the program of the 9th this invention supportand is an available recording medium by computer.

[0023]

[Mode for carrying out the invention]Hereafterit explainsreferring to Drawings for an embodiment of the invention.

[0024]Drawing 1 is a figure showing the outline of the composition of the copyright management system of this invention. In drawing 11 is an electronic music distribution (EMD) serverand 2 an Internet line and 3The personal computer of the users who have predetermined host ID which is an example of the host device of this inventionand 4 are playback apparatus CD-R and whose 5 are examples of the playback equipment of this inventionby which it is not connected to Internet line 2

and which has individual predetermined apparatus ID. In drawing 1the apparatus Athe apparatus Band the apparatus C are shown as the playback apparatus 5reproduction is permitted to the apparatus A and the apparatus C and the state where reproduction is not permitted is shown in the apparatus B. Each playback apparatus 5 is composition connectable with the personal computer 3 with a telecommunication cable.

[0025]Nextthe outline of operation of such a copyright management system is explained. Firsta user downloads contents data via Internet line 2 with users' personal computer 3 from EMD server 1. The personal computer 3 enciphers the downloaded contents data by a predetermined methodand copies to CD-R4. At this timeit may be copied to two or more CD-R4 with the personal computer 3and CD-R4 of one sheet created may be copied to two or more CD-R4. A user inserts CD-R4 in the apparatus A or the apparatus C which is the playback apparatus 5 decided beforehand. The apparatus A or the apparatus C permitted reproduction can reproduce desired contents. At this timeeven if a user inserts CD-R4 in the apparatus B by which reproduction is not permitteddesired contents are unreproducible. Thusthe contents data copied to CD-R4 whose points of the copyright management system of this invention are general-purpose media is renewable only with the playback apparatus 5 in which it was enciphered by the original system of the personal computer 3and reproduction was permitted beforehand.

[0026]Drawing 2 shows the outline of operation that contents data is not reproduced only to the predetermined playback apparatus 5. The personal computer 3 has ID001 as host ID. The playback apparatus 5 has ID00A as apparatus ID. And the personal computer 3 enciphers desired contents data by a predetermined method to CD-R4and gives ENC001 which is encryption ID using host ID. That isthe enciphered contents 6 which have ENC001 are recorded on CD-R4. The personal computer 3 generates the decode key 7 which is an example of the decoding information on this invention in one side. This decode key 7 has ID00A which is DEC001 which is ID for decoding created using host ID for decoding the enciphered contentsand apparatus ID of the playback apparatus 5. And the decode key 7 is transmitted to the playback apparatus 5 from the personal computer 3.

[0027]A user inserts CD-R4 in which the enciphered contents were accommodated in the playback apparatus 5. The playback apparatus 5 verifies whether ENC001 contained in the enciphered contents and DEC001 which are contained in the decode key correspond. It is verified whether apparatus ID00A contained in the decode key 7 and apparatus ID00A of playback apparatus 5 which is apparatus ID peculiar to the playback apparatus 5 correspond. In verification of above bothwhen correspondence and coincidence are obtainedthe playback apparatus 5 can reproduce desired contents by decrypting the enciphered contents which are contained in CD-R4.

[0028]Drawing 3 is a block diagram showing an example of the composition of the personal computer 3. 22 is a means of communication for receiving distribution of the

contents enciphered by the general-purpose encryption method in EMD server 1 via Internet line 2and 23It is a contents acquiring means for acquiring the contents enciphered from said means of communication 228 is a decoding means for decoding the enciphered contents which came to hand with a general-purpose decoding method9 is a contents encryption means which enciphers the decrypted contents using ID for encryptionand 10 is a recording device for recording the enciphered contents on CD-R4.

[0029]14 is the self-ID holding mechanism holding host IDand 15 is a self-ID acquiring means for acquiring host ID from the self-ID holding mechanism 1416 is ID for codes from host ID and ID for decoding which were acquired ID creating means for ID decoding for codes for generatingand 17Are a decode key creating means for generating a decode key using ID generated by the ID creating means 16 for ID decoding for codesand ID generated by the apparatus ID acquiring means 20and 18It is a decode key issuing means for publishing the decode key generated by the decode key creating means 17 to the playback apparatus 5.

[0030]11 is a key acquiring means for the number information 38 (after-mentioned) to come to hand from 1 via the means of communication 2213 is a lock management information control meansand 12 is a lock management information database.

[0031]19 is a means of communication for communicating with the playback apparatus 520 is an apparatus ID acquiring means for apparatus ID to come to hand from the playback apparatus 5 via the means of communication 19and 21 is a decode key deleting means for deleting the decode key published by the playback apparatus 5.

[0032]Above-mentioned ID creating means 16 for ID decoding for codesdecode key creating means 17decode key issuing means 18and decode key deleting means 21 correspond as an example of the selection indication means of this invention.

[0033]Drawing 4 is a block diagram showing an example of composition of the playback apparatus 5. In drawing 424 is a media drive for driving CD-R4and 25It is ID extraction means for codes for extracting ID for codes from contents recorded on CD-R4 set to the media drive 2426 is a means of communication for communicating with the personal computer 3and 27 is the decode key holding mechanism for holding the decode key 7 published with the personal computer 328 is a decode key acquisition means for acquiring the decode key 7 from the means of communication 26 or the decode key holding mechanism 2737 is ID extraction means for decoding for extracting ID for decoding from the decode key acquisition means 2830 is an apparatus ID extraction means for extracting apparatus ID from the decode key 7 acquired in the decode key acquisition means 2831 is the apparatus ID holding mechanism for holding apparatus ID peculiar to each playback apparatus 5and 33 is an apparatus ID comparison means for comparing apparatus ID acquired in apparatus ID acquiring means 32 with apparatus ID extracted in the apparatus ID extraction means 30.

[0034]From the comparison result in a codethe ID comparison means 29 for

decodingand the apparatus ID comparison means 3334. It is a reproduction propriety judging means which judges whether it is possible to reproduce desired contents in the playback apparatus 535 is a decode processing means for decoding the enciphered contents data which is supplied from the media drive 24 based on the decided result in the reproduction propriety judging means 34and 36 is an output means for carrying out the reproducing output of the contents by which decoding processing was carried out in the decode processing means 35.

[0035]Nextthe details of operation of the copyright management system of this invention of the above composition are explainedreferring to drawing 5 and drawing 6. Drawing 5 is a figure explaining the operation in the copyright management whole system. Drawing 6 is a flow chart of the whole copyright management system of this invention.

[0036]Firsta user demands distribution of the number information 38 via Internet line 2. That isadmission in service is required of the EMD server 1 side (Step 101). Information on the number of a reproducing permission of the playback apparatus 5 for which a user wishes is included in this demand. In EMD server 1when accepting a user's subscriptionthe number information 38 is distributed via Internet line 2 (Step 102). In this number information 38the number of a reproducing permission of an individual user who wishes to register as a club member is contained.

[0037]And when a user wishes distribution of contentsthe personal computer 3 transmits a distribution request of desired contents to EMD server 1 via Internet line 2 (Step 103). EMD server 1 will transmit contents data and the number information 38 which enciphered contents for which a user asks with a general-purpose encryption method to the personal computer 3 via Internet line 2if a contents distribution demand is received (Step 104). The personal computer 3 will decode contents data and the number information 38 which were enciphered by a general-purpose decoding methodif contents data and the number information 38 which were enciphered are received.

[0038]If CD-R4 is set to the personal computer 3 by user and predetermined operation is carried outthe personal computer 3 will encipher using host IDand will record decrypted contents on CD-R4 (Step 105).

[0039]And when reproducing CD-R4 on which contents as which a user was enciphered were recorded in the playback apparatus 5the playback apparatus 5 performs issue requesting of the decode key 7 first (Step 106). When the playback apparatus 5 has the decode key 7and when applying a trigger from the personal computer 3 to the playback apparatus 5this step 106 becomes unnecessary.

[0040]The personal computer 3 will advance a Request to Send of apparatus ID of the playback apparatus 5 to the playback apparatus 5if issue requesting of the decode key 7 is received from the playback apparatus 5 (Step 107). If the playback apparatus 5 receives a Request to Send of apparatus IDthe playback apparatus 5 will send apparatus ID peculiar to the playback apparatus 5 to the personal computer 3 (Step

108). And the personal computer 3 generates the decode key 7 from ID00A which is apparatus ID peculiar to DEC001 and the playback apparatus 5 which are ID for decoding generated from host ID peculiar to the personal computer 3. And the personal computer 3 sends the generated decode key 7 to the playback apparatus 5 (Step 109).

[0041]When a user is going to reproduce desired contents in the playback apparatus 5the playback apparatus 5 advances a reproduction request of enciphered content to CD-R4 (Step 110). In the playback apparatus 5ENC001 recorded on the contents 6 as which CD-R4 was enciphered is compared with DEC001 which are contained in the decode key 7 transmitted from the personal computer 3and it verifies that it is that to which both correspond. That isit verifies that 001 which is host ID is in agreement in both. It is verified whether ID00A which is apparatus ID contained in the decode key 7and ID00A of playback apparatus 5 which is apparatus ID peculiar to the playback apparatus 5 correspond. And if it is checked that conditions of above both are fulfilledthe playback apparatus 5 will decrypt the enciphered contents 6and will reproduce desired contents (Step 111).

[0042]In drawing 5the portion by which the center section was surrounded shows the processing in the dedicated software for exchanging the data of EMD server 1 and the personal computer 3. The portion surrounded in the lower right in the figure direction shows the processing in the dedicated software for exchanging the data between the playback apparatus 5 and the personal computer 3. In such dedicated softwaresince processing is performed protecting the data of a key etc. so that it may not be accessed from the outsidethe information transmitted and received is not revealed outside.

[0043]Drawing 7 is the flow chart which illustrated operation of the personal computer 3 in the above-mentioned copyright management system. Operation of the personal computer 3 is explained belowreferring to drawing 3 and drawing 7.

[0044]Drawing 7 (a) is a flow when copying desired contents data to CD-R4. A user starts operation of the personal computer 3 first (Step 210). And the personal computer 3 demands determination of whether to newly purchase the number information 38 from a user (Step 211). When judging that the number information 38 is purchasedthe personal computer 3 carries out purchase processing of the number information 38 (Step 212)and the lock management information control means 13 of the personal computer 3 registers lock management information into the lock management information database 12 (Step 213). The number information 38 already existsand when it is not newly necessary to purchaseit progresses to the following step.

[0045]In Step 213if lock management information is registeredthe personal computer 3 will demand determination of whether to purchase contents next from a user (Step 214). If it is determined that contents are purchasedthe contents acquiring means 23 of the personal computer 3 will perform purchase processing of contents via the

means of communication 22 (Step 215). Processing is ended when it is determined that contents are not purchased (Step 218). If content purchase processing is completed in Step 215the decoding means 8 will decrypt contents enciphered with a general-purpose decoding method. And the contents encryption means 9 enciphers contents using ID for codes generated by the ID creating means 16 for ID decoding for codes (Step 216)The recording device 10 copies enciphered contents to CD-R4 (Step 217)and ends processing (Step 218).

[0046]Drawing 7 (b) is a flow in case the personal computer 3 generates a decode key to the playback apparatus 5 by which the reproducing permission was carried out. Firstthe personal computer 3 makes the issue processing of a decode key start (Step 220). And the personal computer 3 issues the directions which acquire the decode key 7 from the playback apparatus 5 (Step 221). Nextthe personal computer 3 verifies whether the playback apparatus 5 has the decode key 7 (Step 222). When the playback apparatus 5 has already had the decode key 7it is judged whether the decode key 7 is deleted (Step 223). Processing is ended when not deleting the decode key 7 (Step 230). When the playback apparatus 5 does not have the decode key 7the personal computer 3 progresses to the following step. In the following stepthe lock management information control means 13 obtains lock management information from the lock management information database 12 (Step 225)and passes it to the decode key creating means 17.

[0047]On the other handthe apparatus ID acquiring means 20 acquires apparatus ID from the playback apparatus 5 via the means of communication 19 (Step 226)and it is judged whether issue of the decode key 7 is appropriate for the decode key creating means 17 (Step 227). Processing is ended when issue of the decode key 7 is not appropriate (Step 230). When issue of the decode key 7 is appropriatethe decode key creating means 17 generates the decode key 7 from ID for decoding obtained from the ID creating means 16 for ID decoding for codesand apparatus ID acquired from the playback apparatus 5 (Step 228). And the decode key issuing means 18 transmits the decode key 7 to the playback apparatus 5and ends processing (Step 229) (Step 230).

[0048]Drawing 7 (c) shows an example of lock management information stored in the lock management information database 12. A situation where the decode key 7 is published to one set of the playback apparatus 5 in which a user has got three sets of the number of a reproducing permission from EMD server 1and this lock management information has ID of ID00A is shown. An acquisition day of a key and the date of issue of the decode key 7 are recorded on this lock management information.

[0049]Drawing 8 shows a process flow by the side of the playback apparatus 5. Step 341 in drawing 8 (a) - Step 344 are equivalent to Step 106 in drawing 6 - Step 109. An operation flow of the playback apparatus 5 is explained belowreferring to drawing 8 and drawing 4.

[0050]In drawing 8 (a)the playback apparatus 5 starts processing of a decode key

demand first (Step 340). The means of communication 26 transmits the issue requesting of the decode key 7 to the personal computer 3 side (Step 341). If transmission of apparatus ID of the playback apparatus 5 is required from the personal computer 3 sidethe decode key acquisition means 28 will transmit apparatus ID currently held at the apparatus ID holding mechanism 31 to the personal computer 3 side via the means of communication 26 (Step 342). If a decode key is published from the personal computer 3the means of communication 26 receives the published decode key 7 (Step 343)and the decode key acquisition means 28 will register the acquired decode key 7 into the decode key holding mechanism 27 (Step 344)and it will end processing (Step 345).

[0051]Drawing 8 (b) is an operation flow figure at the time of reproducing contents in the playback apparatus 5.

[0052]Firstthe playback apparatus 5 starts contents playback processing by a user's operation (Step 350). The decode key acquisition means 28 checks whether the decode key holding mechanism 27 possesses the decode key 7 (Step 351). When the decode key 7 does not exist in the decode key holding mechanism 27it progresses to the step of whether to acquire the decode key 7 (Step 352). In this step 352when not acquiring the decode key 7processing is ended (Step 361)and when acquiring the decode key 7it progresses to the decode key demand flow shown in drawing 8 (a) (Step 353). When the decode key 7 exists in the decode key holding mechanism 27apparatus ID and apparatus ID of the playback apparatus 5 which are contained in the decode key 7 are compared (Step 354). Namelythe apparatus ID extraction means 30 extracts apparatus ID from the decode key 7 which exists in the decode key acquisition means 28and passes it to the apparatus ID comparison means 33. Apparatus ID acquiring means 32 acquires peculiar apparatus ID which exists in the apparatus ID holding mechanism 31and passes it to the apparatus ID comparison means 33. And it is compared whether apparatus ID passed from the apparatus ID extraction means 30 and apparatus ID of the apparatus ID comparison means 33 passed from apparatus ID acquiring means 32 correspond (Step 355). Processing is ended when both apparatus ID is not in agreement (Step 361).

[0053]When both apparatus ID is in agreementID extraction means 25 for codes acquires ID for codes contained in contents from the media drive 24 (Step 356)and passes it to a code and the ID comparison means 29 for decoding. On the other handID extraction means 37 for decoding extracts ID for decoding from the decode key 7 which exists in the decode key acquisition means 28and passes it to a code and the ID comparison means 29 for decoding. And a code and the ID comparison means 29 for decoding compare ID for codes acquired from enciphered contents with ID for decoding contained in the decode key 7 (Step 357). That isa code and the ID comparison means 29 for decoding compare ID for codes with ID for decodingand both verify whether it is a thing corresponding to the same host ID (Step 358).

[0054]When above-mentioned ID for codes and ID for decoding do not correspondthe

reproduction propriety judging means 34 carries out a judgment of being unreproducibleand ends processing (Step 361). When it is that to which both ID correspondstake out the reproduction propriety judging means 34 and a renewable judgment the decode processing means 35Decrypting the enciphered contents 6 using the decode key 7 (Step 359) by outputting decrypted contentsthe output means 36 reproduces contents for which a user asks (Step 360)and ends processing (Step 361).

[0055]Drawing 9 is a mimetic diagram showing the whole copyright management system of this invention in case there is two or more sets of the playback apparatus 5 by which the reproducing permission was carried out. In the example shown in drawing 9the case where two setsthe apparatus A which is a portable CD player among the playback apparatus 5and the apparatus B which is minicomponentshave obtained the reproducing permission is shown. In such a caseas ID for decodingthe personal computer 3 generates the decode key 7 which has ID00A as DEC001 and apparatus ID to the apparatus Aand generates to it the decode key 7 which has 00B as DEC001 and apparatus ID as ID for decoding at the apparatus B. And these decode keys 7 are transmitted to the apparatus A and the apparatus Brespectively.

[0056]Herein order to reproduce the enciphered contents 6 by the apparatus Aand in order to reproduce by the apparatus Btwo CD-R4 are copied in the personal computer 3. At this timethe enciphered same contents 6 are recorded on each CD-R4. That isENC001 is stored in the enciphered contents 6 as a key for codes with the enciphered same contents data.

[0057]The apparatus A and the apparatus B decrypt the contents 6 enciphered with the decode key 7 which each hasand reproduce desired contents.

[0058]Drawing 10 illustrates a variation from which copyright is protected by a copyright management system of this invention by composition to the aboveand operation.

[0059]In drawing 10a case where another different personal computer 43 exists is shown in the personal computer 3 as a host device. Three setsthe apparatus Athe apparatus Band the apparatus Cexist as the playback apparatus 5among these the apparatus A shows the state that the decode key 7 was published with the personal computer 3 and of being the playback apparatus 5.

[0060]On the above conditionsa case where illegal acquisition of the CD-R on which contents were first recorded with the personal computer 43 which is a third party's personal computer is carried out is considered. In this casethe personal computer 43 enciphers contents to CD-R4 inserted in the personal computer 43 using ID002 which is host ID of the personal computer 43and ENC002 is contained in the enciphered contents 46 as an encryption key. If a user is going to reproduce desired contents using the apparatus AWhen it has the contents 46 as which CD-R4 was enciphered (i.e.when ENC002 exists in the enciphered contents 46)the apparatus A. As mentioned aboveDEC001 which is ID for decoding contained in the decode key 7 which the apparatus A has is compared with ENC002 which are contained in the enciphered

contents 46and both check not originating in the same host ID. Thereforethe apparatus A cannot reproduce contents obtained by CD-R recorded with the personal computer 43 in this way coming to hand unjustly.

[0061]Nextsupposing the decode key 7 is not published by the apparatus Bthe apparatus B can reproduce neither the contents copied with the personal computer 3nor the contents copied with the personal computer 43though natural.

[0062]Nextthe apparatus C assumes that it does not have the regular decode key 7but has what copied the decode key 7 of the apparatus A unjustly. In that casesince peculiar apparatus ID which the apparatus C has is ID00C and apparatus ID which exists in the decode key 7 copied illegally by one side is ID00Ait is judged that apparatus ID of apparatus C of both does not correspond. Thereforein the apparatus C which copied the decode key 7 illegallydesired contents are unreproducible. Of coursethe contents copied illegally with the personal computer 43 are also unreproducible.

[0063]Drawing 11 is the figure which made the list the range from which copyright is protected as mentioned above at a case. That isthe playback apparatus 5 is apparatus which has the regular decode key 7 by which the reproducing permission was carried outand only when CD-R4 is copied with a user's regular personal computer 3the contents for which a user asks can be reproduced. Howeversuch contents cannot be reproducedwhen the playback apparatus 5 is apparatus which does not have the decode key 7and when the playback apparatus 5 is apparatus which has copied the decode key 7 illegally.

[0064]Drawing 12 is a figure showing a flow when changing the playback apparatus 5 by which the reproducing permission was carried out without changing the number of a reproducing permission of the playback apparatus 5.

[0065]For examplethe user shall have three sets of the playback apparatus 5the apparatus Athe apparatus Band the apparatus Camong these the reproducing permission shall be made by two setsthe apparatus A and the apparatus B. And the number of a reproducing permission of two sets makes an example the case where reproducing permission apparatus is changed into the apparatus B and the apparatus C from the apparatus A and the apparatus B without changingand a user explains operation of the copyright management system of this embodiment in that case below.

[0066]In drawing 12Step 401 is equivalent to Step 101 - Step 104 which are shown in drawing 6. Step 402 corresponds to 105 shown in drawing 6and Step 403 - Step 406 are equivalent to Step 106 - Step 109 which are shown in drawing 6. The operation corresponding to Step 403 - Step 406 in Step 407 - Step 410 is made between the personal computer 3 and the apparatus B. In the apparatus A and the apparatus Boperation can reproduce so far the contents for which a user asks in the state of ** practice ****** (Step 411Step 412). Howeverthe apparatus C which does not have the decode key 7 cannot reproduce contents (Step 413).

[0067]Nextthe personal computer 3 advances a Request to Send so that the decode

key 7 which the apparatus A has may be transmitted to the apparatus A (Step 414). And if the apparatus A receives the Request to Send of the decode key 7 from the personal computer 3the decode key 7 which the apparatus A has will be transmitted to the personal computer 3and the decode key 7 will be deleted from the apparatus A (Step 415). The decode key 7 of the apparatus A received also in the personal computer 3 is deleted by the decode key deleting means 21 (Step 224 (refer to drawing 7 (b))).

[0068]And between the apparatus C and the personal computer 3the decode key 7 is transmitted to the apparatus C in Step 416 – Step 419 by the same processing as Step 403 – Step 406. As a resultby the apparatus Adesired contents cannot be reproduced (Step 420) but desired contents can be reproduced in the apparatus B and the apparatus C (Steps 421 and 422).

[0069]As mentioned aboveaccording to the copyright management system of carrying of this embodimentsince two or more sheet copy is possible to general-purpose CD-R4desired contentsWhen reproducing with two or more playback apparatus 5a portable playera minicomponenta car stereoetc. can be set to each playback apparatus 5and do not need to apply the time and effort which carries CD-R4 one by one.

[0070]According to the copyright management system of this embodimentby restricting the number of the playback apparatus 5 reproduced instead of what restricts a duplicate of CD-R4although protection of copyright is aimed ata user's convenience can be raised.

[0071]Since EMD server 1 does not need to perform license management of the individual playback apparatus 5 and should manage only the number of licence of the playback apparatus 5it can be managed with an easy system configuration also for the EMD server 1 side.

[0072]Since the decode key 7 for decoding desired contents is published in users' personal computer 3the user does not need to ask the EMD server 1 side one by oneand can enjoy desired contents by easy processing.

[0073]Although explanation to the above is related with a copyright management system of this inventiona copyright management method using a system of the above-mentioned composition is also the range of this invention.

[0074]In explanation to the abovealthough distribution of the number information 38 from EMD server 1 in Step 101 to the personal computer 3 presupposed that it is made via Internet line 2it may be transmitted or sentfor example by other methodssuch as mail.

[0075]Although it presupposed that the personal computer 3 and the playback apparatus 5 are connected with a telecommunication cableand an exchange of the decode key 7 etc. are made in explanation to the abovethe personal computer 3 and the playback apparatus 5 may be composition connected not by a cable but by radio. It may be the composition that an exchange of the decode key 7 etc. are made using

physical mediasuch as CD-R. In that casethe exchange of the decode key 7 grade between the personal computer 3 and the playback apparatus 5 serves as operation instead of transmission or reception sent or received. The effect same also in such a case as the above can be acquired.

[0076]Although they presupposed that it is CD-Reven if the media on which the enciphered contents are recorded in explanation to the above are other medianaturally they are good.

[0077]Although the personal computer 3 presupposed that the decode key 7 is published to the playback apparatus 5 within the number by which the reproducing permission was carried out in explanation to the abovethere may be a function to restrict issue of the decode key 7 to still more specific apparatus. As such an exampleit may be the composition of publishing the decode key 7 only to the playback apparatus 5 corresponding to high-quality soundfor example.

[0078]Not only music data but the information on still picture informationa video dataalphabetic dataand others is included in the contents in explanation to the above. That isthe distributing server of this invention may be a server which is not limited to EMD server 1 but can distribute above various contents.

[0079]Although it presupposed that the host devices of this invention are the personal computers 3 and 43 in explanation to the aboveas long as the host device of this invention can achieve the above-mentioned functionthey may be apparatus other than a personal computer. Although a cellular phonea personal digital assistantetc. are mentioned as such an exampleit is not limited to these.

[0080]Although the playback apparatus 5 explained the example which is one set or three sets by explanation to the aboveif the playback apparatus 5 is less than the number of a reproducing permissionit cannot be overemphasized that they may be how many sets. What is necessary is just to notify change of the number of a reproducing permission to the distributing server side in Step 101 shown in drawing 6 to change the number of a reproducing permission.

[0081]The program of this invention is a program for performing the function of all or a part of means (or equipmentan elementetc.) of the copyright management systems of this invention mentioned above by computerand is a program which collaborates with a computer and operates.

[0082]All or a part of means (.) of the copyright management systems of this invention which the recording medium of this invention mentioned above Or it is the recording medium which supported the program for performing the function of all or the parts of equipmentan elementetc. by computerand said program which reading was possible and was read by computer is a recording medium which cooperates with said computer and performs said function.

[0083]The above "some means (or equipmentan elementetc.)" of this invention means one or some means of two or more of those meansand the above "some steps (or a processoperationan operationetc.)" of this invention means one or some steps of two

or more of those steps.
[0084]The above "function of MEANS (or equipmentan elementetc.)" of this invention means the function of all or a part of said meansand the above "operations (or a processoperationan operationetc.) of a step" of this invention means operation of all or a part of said steps.
[0085]One usage pattern of the program of this invention may be a mode which is recorded on the recording medium which can be read by computercollaborates with a computerand operates.
[0086]One usage pattern of the program of this invention may be a mode which transmits the inside of a transmission mediumis read by computercollaborates with a computerand operates.
[0087]As a data structure of this inventionthe kind of a databasea data formata data tablea data listand dataetc. are included.
[0088]As a recording mediumROM etc. are contained and transmission mediasuch as the Internetlightan electric wavea sound waveetc. are contained as a transmission medium.
[0089]The computer of this invention mentioned above may contain not only hardware with pure and simple CPU etc. but firmwareand OS and also peripheral equipment.
[0090]As explained aboveit may realize by software and composition of this invention may be realized in hardware.
[0091]
[Effect of the Invention]According to this inventionthe user-friendly copyright protection system for a userthe copyright protection methodits host deviceits programand the recording medium that supported the program can be provided.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]Drawing 1 is a figure showing the outline of the copyright management system of an embodiment of the invention.
[Drawing 2]Drawing 2 is a figure showing the outline of operation of the copyright management system of an embodiment of the invention.
[Drawing 3]Drawing 3 is a block diagram showing the composition of the personal computer which constitutes the copyright management system of an embodiment of the invention.
[Drawing 4]Drawing 4 is a block diagram showing the composition of the playback apparatus which constitutes the copyright management system of an embodiment of the invention.
[Drawing 5]Drawing 5 is a schematic view showing operation of the whole copyright management system of an embodiment of the invention.

[Drawing 6]Drawing 6 is a flow chart showing operation of the whole copyright management system of an embodiment of the invention.
[Drawing 7]Drawing 7 is a flow chart showing operation of the personal computer which constitutes the copyright management system of an embodiment of the invention.
[Drawing 8]Drawing 8 is a flow chart showing operation of the playback apparatus which constitutes the copyright management system of an embodiment of the invention.
[Drawing 9]Drawing 9 is a schematic view showing operation of the whole copyright management system of an embodiment of the invention.
[Drawing 10]Drawing 10 is a figure showing the variation of the copyright protected by the copyright management system of an embodiment of the invention.
[Drawing 11]Drawing 11 is a figure showing the variation of the copyright protected by the copyright management system of an embodiment of the invention.
[Drawing 12]Drawing 12 is a flow chart showing the operation at the time of making a number change of a reproducing permission of the playback apparatus which constitutes the copyright management system of an embodiment of the invention.
[Drawing 13]Drawing 13 is a schematic view of the copyright management system of conventional technology.
[Drawing 14]Drawing 14 is a schematic view of the copyright management system of conventional technology.
[Explanations of letters or numerals]
1 EMD server
2 Internet line
3 and 43 A personal computer
4 CD-R
5 Playback apparatus
6 Enciphered contents
7 A decode key
8 A decoding means
9 A contents encryption means
10 A recording device
11 A key acquiring means
12 A lock management information database
13 A lock management information control means
14 Self-ID holding mechanism
15 A self-ID acquiring means
16 ID creating means for ID decoding for codes
17 A decode key creating means
18 A decode key issuing means
1922and 26 A means of communication

20 An apparatus ID acquiring means
21 A decode key deleting means
23 A contents acquiring means
24 A media drive
25 ID extraction means for codes
27 Decode key holding mechanism
28 A decode key acquisition means
29 An ID comparison means for cipher items
30 An apparatus ID extraction means
31 Apparatus ID holding mechanism
32 An apparatus ID acquiring means
33 An apparatus ID comparison means
34 A reproduction propriety judging means
35 Decode processing means 36 An output means
37 ID extraction means for decoding
38 A key

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2003－323351
（P2003－323351A）
(43)公開日　平成15年11月14日(2003.11.14)

(51)Int.Cl.[7]	識別記号	Ｆ１		ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｆ	５Ｂ０１７
			３２０Ｅ	５Ｄ０４４
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ	５Ｄ１１０
20/12		20/12		５Ｊ１０４
27/00		27/00	Ｄ	

審査請求　未請求　請求項の数10　ＯＬ　（全 16 頁）　最終頁に続く

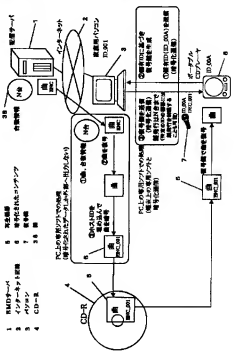
(21)出願番号　特願2003－50043(P2003－50043)
(22)出願日　平成15年２月26日(2003.2.26)
(31)優先権主張番号　特願2002－50963(P2002－50963)
(32)優先日　平成14年２月27日(2002.2.27)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　宮本　晴敏
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100092794
弁理士　松田　正道

最終頁に続く

(54)【発明の名称】　著作権管理システム、著作権管理方法、ホスト装置、プログラムおよび記録媒体

(57)【要約】
【課題】　ユーザにとって使い勝手がよい著作権保護システム、著作権保護方法、そのホスト装置、そのプログラム、そのプログラムを担持した記録媒体を提供すること。
【解決手段】　所定のコンテンツを所定の暗号化方法で暗号化するとともに、あらかじめ再生を許可された再生装置５の台数に応じて、特定の再生装置５を選択し、前記選択された特定の再生装置５へ、前記暗号化されたコンテンツ６を復号化するための復号鍵等の復号化情報を送るホスト装置。



【特許請求の範囲】
【請求項１】　所定のコンテンツを所定の暗号化方法で暗号化するとともに、再生を許可された再生装置の台数に応じて、特定の再生装置を選択し、前記選択された特定の再生装置へ、前記暗号化されたコンテンツを復号化するための復号化情報を送るホスト装置。
【請求項２】　前記選択を指示するための選択指示手段をさらに備える、請求項１に記載のホスト装置。
【請求項３】　前記暗号化は、前記ホスト装置に固有のホストＩＤを利用したものであり、
前記復号化情報には、前記特定の再生装置の機器ＩＤと、前記ホストＩＤが含まれている、請求項１に記載のホスト装置。
【請求項４】　前記所定のコンテンツおよび前記台数の情報は、配信サーバから暗号化されて配信されたものである、請求項１に記載のホスト装置。
【請求項５】　ホスト装置により暗号化されたコンテンツが有するホストＩＤと、前記復号化情報に含まれているホストＩＤとが一致し、かつ、前記復号化情報に含まれる機器ＩＤと、固有の機器ＩＤとが一致していることを条件として、前記暗号化されたコンテンツを再生する再生装置であって、
前記ホスト装置は、所定のコンテンツを固有のホストＩＤを利用して暗号化するとともに、再生を許可された再生装置の台数に応じて、特定の再生装置を選択し、前記選択された特定の再生装置へ、前記暗号化されたコンテンツを復号化するための、前記特定の再生装置の機器ＩＤおよび前記ホストＩＤが含まれている復号化情報を送る、再生装置。
【請求項６】　前記再生装置は、インターネットに接続されていない、請求項５に記載の再生装置。
【請求項７】　所定のコンテンツを配信する配信サーバと、
所定のコンテンツを所定の暗号化方法で暗号化するホスト装置と、
前記暗号化されたコンテンツを再生する再生装置と、を備え、
前記ホスト装置は、再生を許可された再生装置の台数に応じて、特定の前記再生装置を選択し、前記選択された特定の再生装置へ、前記暗号化されたコンテンツを復号化するための復号化情報を送り、
前記再生装置は、前記送られた復号化情報を利用して、前記暗号化されたコンテンツを再生する著作権管理システム。
【請求項８】　所定のコンテンツを配信する配信サーバと、
前記所定のコンテンツを所定の暗号化方法で暗号化するホスト装置と、
前記暗号化されたコンテンツを再生する再生装置と、を備える著作権管理システムを利用した著作権管理方法であって、
前記ホスト装置は、再生を許可された前記再生装置の台数に応じて、特定の前記再生装置を選択し、前記選択された特定の再生装置へ、前記暗号化されたコンテンツを復号化するための復号化情報を送り、
前記再生装置は、前記送られた復号化情報を利用して、前記暗号化されたコンテンツを再生する著作権管理方法。
【請求項９】　請求項７に記載の著作権管理システムの、
所定のコンテンツを所定の暗号化方法で暗号化するホスト装置と、
前記暗号化されたコンテンツを再生する再生装置と、をコンピュータとして機能させるためのプログラム。
【請求項１０】　請求項９に記載のプログラムを担持させた記録媒体であって、コンピュータで利用可能な記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、コンテンツの著作権のライセンス管理を行う著作権管理システム、著作権管理方法、そのホスト装置、そのプログラム、およびそのプログラムの記録媒体に関する。
【０００２】
【従来の技術】近年、ＣＤ－ＤＡのみならず、ｍｐ３（ｍｐｅｇ　ａｕｄｉｏ　ｌａｙｅｒ３）のような元の音源から複製された音楽形式がユーザーに広く利用されている。しかし、ｍｐ３などには著作権管理の方法が確立していないため著作権者にとって大きな問題となっており、これを解決しようとする手段が提案されている。また音楽だけでなく、映像や画像といったデジタルコンテンツについても著作権管理の方法が検討されている。例えば、パソコン上で用いられるＷＭＡ（Ｗｉｎｄｏｗｓ（登録商標）　Ｍｅｄｉａ　Ａｕｄｉｏ）という音楽圧縮方式の著作権管理においてはＤＲＭ（Ｄｉｇｉｔａｌ　Ｒｉｇｈｔ　Ｍａｎａｇｅｍｅｎｔ）と呼ばれる方式が採用されている。これは、暗号化された音楽の復号化には、暗号化した装置の固有ＩＤが必要となる方式であり、暗号化装置と再生装置を同一の装置に限定することで違法コピーの蔓延を防ぐことができる。また、携帯電話等の小型端末をターゲットとした情報配信システムにおいても、配信情報の著作権を保護する方式が提案されている（例えば、特許文献１参照）。配信サーバから配信された情報と配信先の携帯電話の固有ＩＤとを、サーバー上の管理データベースに登録しておき、登録された携帯電話でしか情報を再生できない仕組みとなっている。
【０００３】
【特許文献１】特開２００１－７８２６６号公報
【０００４】

【発明が解決しようとする課題】しかし、それぞれの装置がネットワーク上のサーバーにアクセスできることが前提となるため、ネットワーク接続を前提としない再生装置などで実現できるものではない。

【０００５】また、直接ネットワークにアクセスできない再生装置で著作権のライセンス管理を行う方法として、図１３に示す方法がある。図１３において、１０１は、電子音楽配信（ＥＭＤ）サーバであり、１０２はインターネット回線、１０３はユーザ側のパソコン、１０４は固有ＩＤをもつメディア、例えばＳＤカード（Ｓｅｃｕｒｅ　Ｄｉｇｉｔａｌカード）、１０５は、インターネット回線に接続されていない汎用再生機器１０５である。

【０００６】ここで、パソコン１０３とＳＤカード１０４との間は、チェックイン、チェックアウト方式でデータが送受信される。データのチェックイン、チェックアウトとは、データのコピー回数を管理しながらパソコンと外部機器、メディアとの間でデータを送受信することをいう。チェックアウトとは、データをパソコンから外部機器、メディアに転送することをいう。この場合データにチェックアウト（コピー）の制限回数がある場合には、制限回数を超えるチェックアウトはできない。チェックインとは、パソコンから外部機器、メディアに転送されたデータを、それらの外部機器、メディアに残らないように転送元のパソコンに戻すことをいう。なお、この場合、チェックアウトされたデータは転送元のパソコンにしか戻すことができない。しかし、チェックインによりパソコンに戻されたデータは、再びチェックアウトすることができる。

【０００７】この方法によれば、コンテンツをメディアであるＳＤカード１０４の固有ＩＤと一緒に扱うことで、コンテンツのオリジナルと複製を区別して著作権管理を行う。具体的には、認証されたＳＤカード１０４にのみコンテンツのデータをチェックアウトすることにより、データの不正コピーを防止するものである。すなわち、ユーザは、ＥＭＤサーバ１０１からインターネット回線１０２を介してユーザ側のパソコン１０３でコンテンツデータをダウンロードする。ＳＤカード１０４がパソコン１０３に挿入されることにより、パソコン１０３は、ＳＤカード１０４があらかじめ認証されている所定のＩＤが付与されていることを確認する。パソコン１０３は次にパソコン１０３からコンテンツデータをチェックアウトする。そして、所望のコンテンツデータが取り込まれたＳＤカード１０４を汎用再生機器１０５に挿入することにより、汎用再生機器１０５は、所望のコンテンツを再生することができる。

【０００８】しかし、パソコン１０３のチェックアウト、チックインの機能により、所望のコンテンツデータは、所定数以上の複製が不可能である。従って、上記の所望のコンテンツを、ポータブルプレーヤ、ミニコンポ、カーステレオ等複数の汎用再生機器１０５で再生しようとする場合、コンテンツデータが記録されているＳＤカード１０４を持ち運びその都度ＳＤカード１０４を汎用再生機器１０５にセットしなければならない、という不都合がある。また、上記の方法では、ＳＤカード１０４が比較的高価であるため、所定数以内であっても複数の複製を行うことは、それだけ費用がかかってしまい、ユーザに普及しにくいという欠点がある。

【０００９】このように、上記のような著作権管理システムでは、コンテンツ配信業者の保護に手厚く、ユーザーの使い勝手が犠牲になっている側面があった。

【００１０】ＳＤカード１０４を使用する代わりに汎用メディアであるＭＤ１０７を使用する方法を図１４に示す。図１４に示すシステムにおいて、図１３に示すシステムと異なる点は、ＭＤ１０７は、ＩＤ付録音機器１０６を介してパソコン１０３にチェックイン、チェックアウトされる点である。すなわち、ＭＤ１０７に所望のコンテンツデータを取り込むためには、パソコン１０３は、ＩＤ付録音機器１０６を認証し、ＩＤ付録音機器１０６があらかじめ認証されているＩＤが付与されていることを確認した後、所望のコンテンツデータは、パソコン１０３からＩＤ付録音機器１０６を介してＭＤ１０７にチェックアウトされる。

【００１１】このようなシステムによれば、廉価なＭＤ１０７を使用することができるので、複数の複製を行うことはＳＤカード１０４を使用して複製する場合に比べて費用は安くてすむ。しかし、パソコン１０３へのＩＤ付録音機器１０６のチェックイン、チェックアウトには、データの送受信ごとに認証、暗号処理等の手続が必要であることから、ＩＤ付録音機器１０６に高性能な処理回路が必要となっていた。また、認証、暗号処理の負荷が大きく、ユーザが利用しやすいものではなかった。

【００１２】本発明の目的は、上記の課題を考慮して、ユーザにとって使い勝手がよい著作権保護システム、著作権保護方法、そのホスト装置、そのプログラム、そのプログラムを担持した媒体を提供することを目的とする。

【００１３】

【課題を解決するための手段】上記課題を解決するための、第１の本発明は、所定のコンテンツを所定の暗号化方法で暗号化するとともに、再生を許可された再生装置（５）の台数に応じて、特定の再生装置（５）を選択し、前記選択された特定の再生装置（５）へ、前記暗号化されたコンテンツ（６）を復号化するための復号化情報（７）を送るホスト装置である。

【００１４】第２の本発明は、前記選択を指示するための選択指示手段をさらに備える、請求項１に記載のホスト装置である。

【００１５】第３の本発明は、前記暗号化は、前記ホスト装置に固有のホストＩＤを利用したものであり、前記

復号化情報（７）には、前記特定の再生装置（５）の機器ＩＤと、前記ホストＩＤが含まれている、第１の本発明のホスト装置である。

【００１６】第４の本発明は、前記所定のコンテンツおよび前記台数の情報（３８）は、配信サーバ（１）から暗号化されて配信されたものである、第１の本発明のホスト装置である。

【００１７】第５の本発明は、ホスト装置により暗号化されたコンテンツ（６）が有するホストＩＤと、前記復号化情報（７）に含まれているホストＩＤとが一致し、かつ、前記復号化情報（７）に含まれる機器ＩＤと、固有の機器ＩＤとが一致していることを条件として、前記暗号化されたコンテンツ（６）を再生する再生装置であって、前記ホスト装置は、所定のコンテンツを固有のホストＩＤを利用して暗号化するとともに、再生を許可された再生装置（５）の台数に応じて、特定の再生装置（５）を選択し、前記選択された特定の再生装置（５）へ、前記暗号化されたコンテンツ（６）を復号化するための、前記特定の再生装置（５）の機器ＩＤおよび前記ホストＩＤが含まれている復号化情報（７）を送る、再生装置である。

【００１８】第６の本発明は、前記再生装置（５）は、インターネットに接続されていない、第５の本発明の再生装置である。

【００１９】第７の本発明は、所定のコンテンツを配信する配信サーバ（１）と、所定のコンテンツを所定の暗号化方法で暗号化するホスト装置（３）と、前記暗号化されたコンテンツを再生する再生装置（５）と、を備え、前記ホスト装置（３）は、再生を許可された再生装置（５）の台数に応じて、特定の前記再生装置（５）を選択し、前記選択された特定の再生装置（５）へ、前記暗号化されたコンテンツ（６）を復号化するための復号化情報（７）を送り、前記再生装置（５）は、前記送られた復号化情報（７）を利用して、前記暗号化されたコンテンツ（６）を再生する著作権管理システムである。

【００２０】第８の本発明は、所定のコンテンツを配信する配信サーバ（１）と、前記所定のコンテンツ（１）を所定の暗号化方法で暗号化するホスト装置（３）と、前記暗号化されたコンテンツを再生する再生装置（５）と、を備える著作権管理システムを利用した著作権管理方法であって、前記ホスト装置（３）は、再生を許可された前記再生装置（５）の台数に応じて、特定の前記再生装置（５）を選択し、前記選択された特定の再生装置（５）へ、前記暗号化されたコンテンツ（６）を復号化するための復号化情報（７）を利用して、前記暗号化されたコンテンツ（６）を再生する著作権管理方法である。

【００２１】第９の本発明は、第７の本発明の著作権管理システムの、所定のコンテンツを所定の暗号化方法で暗号化するホスト装置（３）と、前記暗号化されたコンテンツ（６）を再生する再生装置（５）と、をコンピュータとして機能させるためのプログラムである。

【００２２】第１０の本発明は、第９の本発明のプログラムを担持させた記録媒体であって、コンピュータで利用可能な記録媒体である。

【００２３】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照しながら説明する。

【００２４】図１は、本発明の著作権管理システムの構成の概要を示す図である。図１において、１は電子音楽配信（ＥＭＤ）サーバであり、２はインターネット回線、３は、本発明のホスト装置の一例である、所定のホストＩＤを有するユーザ側のパソコン、４はＣＤ－Ｒ、５は、本発明の再生装置の一例である、インターネット回線２に接続されていない、個別の所定の機器ＩＤを有する再生機器である。図１においては、再生機器５として機器Ａ、機器Ｂ、機器Ｃが示されており、機器Ａ、機器Ｃには再生が許可され、機器Ｂには再生が許可されていない状態を示している。また、それぞれの再生機器５はパソコン３と通信ケーブルで接続可能な構成である。

【００２５】次に、このような著作権管理システムの動作の概略を説明する。まず、ユーザは、ＥＭＤサーバ１からユーザ側のパソコン３でコンテンツデータをインターネット回線２を介してダウンロードする。パソコン３は、ダウンロードされたコンテンツデータを所定の方法で暗号化してＣＤ－Ｒ４にコピーをする。このとき、パソコン３により複数のＣＤ－Ｒ４にコピーされてもよし、作成された１枚のＣＤ－Ｒ４が複数のＣＤ－Ｒ４にコピーされてもよい。ユーザは、あらかじめ決められている再生機器５である機器Ａまたは機器ＣにＣＤ－Ｒ４を挿入する。再生を許可された機器Ａまたは機器Ｃは、所望のコンテンツを再生することができる。このとき、ユーザが再生が許可されていない機器ＢにＣＤ－Ｒ４を挿入しても所望のコンテンツを再生することができない。このように、本発明の著作権管理システムのポイントは、汎用メディアであるＣＤ－Ｒ４にコピーされたコンテンツデータは、パソコン３の独自の方式で暗号化され、あらかじめ再生が許可された再生機器５でしか再生できないことである。

【００２６】図２は、所定の再生機器５にしかコンテンツデータが再生されないという動作の概要を示す。パソコン３は、ホストＩＤとしてＩＤ００１を有している。再生機器５は、機器ＩＤとしてＩＤ００Ａを有している。そして、パソコン３は、ＣＤ－Ｒ４に所望のコンテンツデータを所定の方法で暗号化し、ホストＩＤを利用した暗号化ＩＤであるＥＮＣ００１を付与する。すなわち、ＣＤ－Ｒ４には、ＥＮＣ００１を有する暗号化されたコンテンツ６が記録されている。パソコン３は、一方で本発明の復号化情報の一例である復号鍵７を生成す

る。この復号鍵７は、暗号化されたコンテンツを復号するためのホストＩＤを利用して作成された復号用ＩＤであるＤＥＣ００１、および再生機器５の機器ＩＤであるＩＤ００Ａを有する。そして、復号鍵７は、パソコン３から再生機器５に送信される。

【００２７】ユーザは、暗号化されたコンテンツが収容されたＣＤ－Ｒ４を再生機器５に挿入する。再生機器５は、暗号化されたコンテンツに含まれているＥＮＣ００１と復号鍵に含まれているＤＥＣ００１が対応するか検証する。また、再生機器５は、復号鍵７に含まれている機器ＩＤ００Ａと、再生機器５に固有の機器ＩＤである機器ＩＤ００Ａが一致するか検証する。上記の両方の検証において、対応および一致が見られた場合は、再生機器５は、ＣＤ－Ｒ４に含まれる暗号化されたコンテンツを復号化することにより、所望のコンテンツを再生することができる。

【００２８】図３は、パソコン３の構成の一例を示すブロック図である。２２は、ＥＭＤサーバ１において汎用的な暗号方法により暗号化されたコンテンツの配信をインターネット回線２を介して受けるための通信手段であり、２３は、前記通信手段２２から暗号化されたコンテンツを取得するためのコンテンツ入手手段であり、８は入手した暗号化されたコンテンツを汎用的な復号方法により復号するための復号手段であり、９は復号化されたコンテンツを暗号化用ＩＤを利用して暗号化するコンテンツ暗号化手段であり、１０は暗号化されたコンテンツをＣＤ－Ｒ４に記録するための記録手段である。

【００２９】１４は、ホストＩＤを保持している自ＩＤ保持手段であり、１５は自ＩＤ保持手段１４からホストＩＤを取得するための自ＩＤ取得手段であり、１６は取得したホストＩＤから暗号用ＩＤおよび復号用ＩＤを生成するための暗号用ＩＤ復号用ＩＤ生成手段であり、１７は、暗号用ＩＤ復号用ＩＤ生成手段１６により生成されたＩＤ、および機器ＩＤ入手手段２０により生成されたＩＤを利用して復号鍵を生成するための復号鍵生成手段であり、１８は、復号鍵生成手段１７により生成された復号鍵を再生機器５に発行するための復号鍵発行手段である。

【００３０】１１は、通信手段２２を介して１から台数情報３８（後述）を入手するための鍵入手手段であり、１３は、鍵管理情報制御手段であり、１２は、鍵管理情報データベースである。

【００３１】１９は、再生機器５と通信するための通信手段であり、２０は、通信手段１９を介して再生機器５から機器ＩＤを入手するための機器ＩＤ入手手段であり、２１は再生機器５に発行された復号鍵を削除するための復号鍵削除手段である。

【００３２】上記の暗号用ＩＤ復号用ＩＤ生成手段１６、復号鍵生成手段１７、復号鍵発行手段１８、および復号鍵削除手段２１は、本発明の選択指示手段の一例として対応する。

【００３３】図４は、再生機器５の構成の一例を示すブロック図である。図４において、２４は、ＣＤ－Ｒ４を駆動するためのメディアドライブであり、２５は、メディアドライブ２４にセットされたＣＤ－Ｒ４に記録されたコンテンツから暗号用ＩＤを抽出するための暗号用ＩＤ抽出手段であり、２６はパソコン３と通信するための通信手段であり、２７はパソコン３により発行された復号鍵７を保持しておくための復号鍵保持手段であり、２８は通信手段２６または復号鍵保持手段２７から復号鍵７を取得するための復号鍵取得手段であり、３７は復号鍵取得手段２８から復号用ＩＤを抽出するための復号用ＩＤ抽出手段であり、３０は復号鍵取得手段２８において取得した復号鍵７から機器ＩＤを抽出するための機器ＩＤ抽出手段であり、３１は各再生機器５に固有の機器ＩＤを保持するための機器ＩＤ保持手段であり、３３は機器ＩＤ取得手段３２において取得された機器ＩＤと機器ＩＤ抽出手段３０において抽出された機器ＩＤとを比較するための機器ＩＤ比較手段である。

【００３４】３４は暗号・復号用ＩＤ比較手段２９および機器ＩＤ比較手段３３における比較結果より、所望のコンテンツを再生機器５において再生することが可能であるかどうかを判定する再生可否判定手段であり、３５は再生可否判定手段３４における判定結果に基づいて、メディアドライブ２４から供給される暗号化されたコンテンツデータを復号するための復号処理手段であり、３６は復号処理手段３５において復号処理されたコンテンツを再生出力するための出力手段である。

【００３５】次に、以上の構成の本発明の著作権管理システムの動作の詳細を図５および図６を参照しながら説明する。図５は、著作権管理システム全体における動作を説明する図である。また図６は、本発明の著作権管理システムの全体のフロー図である。

【００３６】まず、ユーザは、台数情報３８の配信をインターネット回線２を介して要求する。すなわちＥＭＤサーバ１側にサービスへの入会を要求する（ステップ１０１）。この要求には、ユーザが希望する再生機器５の再生許可台数の情報が含まれている。ＥＭＤサーバ１において、ユーザの加入を認める場合は、台数情報３８をインターネット回線２を介して配信する（ステップ１０２）。この台数情報３８の中には、入会を希望する個別のユーザの再生許可台数が含まれている。

【００３７】そして、ユーザがコンテンツの配信を希望する場合は、パソコン３は所望のコンテンツの配信要求をＥＭＤサーバ１にインターネット回線２を介して送信する（ステップ１０３）。ＥＭＤサーバ１はコンテンツ配信要求を受けると、ユーザが所望するコンテンツを汎用的な暗号方法で暗号化したコンテンツデータおよび台数情報３８をパソコン３にインターネット回線２を介して送信する（ステップ１０４）。パソコン３は暗号化さ

れたコンテンツデータおよび台数情報３８を受けると、汎用的な復号方法により暗号化されたコンテンツデータおよび台数情報３８を復号する。

【００３８】ユーザによりＣＤ－Ｒ４がパソコン３にセットされ所定の操作がされると、パソコン３は復号化されたコンテンツをホストＩＤを利用して暗号化し、ＣＤ－Ｒ４に記録する（ステップ１０５）。

【００３９】そして、ユーザが暗号化されたコンテンツが記録されたＣＤ－Ｒ４を再生機器５において再生する場合、再生機器５は、まず復号鍵７の発行要求を行う（ステップ１０６）。なお、再生機器５が復号鍵７を有している場合、および、パソコン３から再生機器５に対してトリガをかける場合は、このステップ１０６は不要となる。

【００４０】パソコン３は、復号鍵７の発行要求を再生機器５から受けると、再生機器５に対して再生機器５の機器ＩＤの送信要求を出す（ステップ１０７）。再生機器５が機器ＩＤの送信要求を受けると、再生機器５はその再生機器５に固有の機器ＩＤをパソコン３に送る（ステップ１０８）。そして、パソコン３は、パソコン３に固有のホストＩＤから生成された復号用ＩＤであるＤＥＣ００１と再生機器５に固有の機器ＩＤであるＩＤ００Ａとから復号鍵７を生成する。そしてパソコン３は、生成された復号鍵７を再生機器５に送る（ステップ１０９）。

【００４１】ユーザが所望のコンテンツを再生機器５において再生しようとする場合は、再生機器５はＣＤ－Ｒ４に対して暗号化コンテンツの再生要求を出す（ステップ１１０）。再生機器５においては、ＣＤ－Ｒ４の暗号化されたコンテンツ６に記録されたＥＮＣ００１とパソコン３から送信された復号鍵７に含まれるＤＥＣ００１とを比較し、両者が対応するものであることを検証する。すなわち、両者においてホストＩＤである００１が一致することを検証する。さらに、再生機器５は復号鍵７に含まれる機器ＩＤであるＩＤ００Ａと再生機器５に固有の機器ＩＤであるＩＤ００Ａとが一致するかを検証する。そして、上記の両方の条件が満たされることが確認されると、再生機器５は、暗号化されたコンテンツ６を復号化し、所望のコンテンツを再生する（ステップ１１１）。

【００４２】図５において、中央部の囲まれた部分は、ＥＭＤサーバ１とパソコン３とのデータのやり取りを行うための専用ソフトにおける処理を示す。また同図における右下方において囲まれた部分は、再生機器５とパソコン３との間のデータのやり取りを行うための専用ソフトにおける処理を示す。これらの専用ソフトでは、鍵などのデータを外部からアクセスされることがないように保護しながら処理が行われているため、送受信した情報が外部に漏洩することはない。

【００４３】図７は、上記の著作権管理システムにおいてパソコン３の動作を説明したフロー図である。図３および図７を参照しながらパソコン３の動作を次に説明する。

【００４４】図７（ａ）は、所望のコンテンツデータをＣＤ－Ｒ４にコピーするときのフローである。ユーザは、まずパソコン３の動作を開始する（ステップ２１０）。そしてパソコン３は、ユーザに台数情報３８を新規購入するかどうかの決定を促す（ステップ２１１）。台数情報３８を購入すると判断する場合は、パソコン３は台数情報３８の購入処理をし（ステップ２１２）、パソコン３の鍵管理情報制御手段１３は鍵管理情報データベース１２に鍵管理情報を登録する（ステップ２１３）。台数情報３８がすでに存在して新規購入する必要がない場合は、次のステップに進む。

【００４５】ステップ２１３において、鍵管理情報が登録されると、パソコン３は次にコンテンツを購入するかどうかの決定をユーザに促す（ステップ２１４）。コンテンツが購入されることが決定されると、パソコン３のコンテンツ入手手段２３は通信手段２２を介してコンテンツの購入処理を行う（ステップ２１５）。コンテンツが購入されないと決定された場合は、処理を終了する（ステップ２１８）。ステップ２１５においてコンテンツ購入処理が完了すると、復号手段８は暗号化されているコンテンツを汎用的復号方法により復号化する。そして、コンテンツ暗号化手段９は、暗号用ＩＤ復号用ＩＤ生成手段１６により生成された暗号用ＩＤを用いてコンテンツを暗号化し（ステップ２１６）、記録手段１０は暗号化されたコンテンツをＣＤ－Ｒ４にコピーして（ステップ２１７）、処理を終了する（ステップ２１８）。

【００４６】図７（ｂ）は、再生許可された再生機器５に対してパソコン３が復号鍵を生成するときのフローである。まず、パソコン３は復号鍵の発行処理を開始させる（ステップ２２０）。そしてパソコン３は、再生機器５から復号鍵７を取得する指示を出す（ステップ２２１）。次にパソコン３は再生機器５が復号鍵７を有しているかどうかを検証する（ステップ２２２）。再生機器５がすでに復号鍵７を有している場合は、復号鍵７を削除するかどうかを判断する（ステップ２２３）。復号鍵７を削除しない場合は、処理を終了する（ステップ２３０）。再生機器５が復号鍵７を有していない場合は、パソコン３は次のステップに進む。次のステップにおいて鍵管理情報制御手段１３は鍵管理情報データベース１２から鍵管理情報を入手し（ステップ２２５）、復号鍵生成手段１７に渡す。

【００４７】一方、機器ＩＤ入手手段２０は、通信手段１９を介して再生機器５から機器ＩＤを取得し（ステップ２２６）、復号鍵生成手段１７は復号鍵７の発行が適切であるかどうかを判断する（ステップ２２７）。もし、復号鍵７の発行が適切でない場合は処理を終了する（ステップ２３０）。復号鍵７の発行が適切である場合

は、復号鍵生成手段１７は暗号用ＩＤ復号用ＩＤ生成手段１６から得た復号用ＩＤと再生機器５から取得した機器ＩＤから復号鍵７を生成する（ステップ２２８）。そして復号鍵発行手段１８は復号鍵７を再生機器５に送信して（ステップ２２９）処理を終了する（ステップ２３０）。

【００４８】図７（ｃ）は、鍵管理情報データベース１２に格納されている鍵管理情報の一例を示す。この鍵管理情報は、ユーザはＥＭＤサーバ１から３台の再生許可台数を得ており、ＩＤ００ＡのＩＤを有する再生機器５の１台に復号鍵７を発行している状況を示している。また、この鍵管理情報には、鍵の入手日と復号鍵７の発行日とが記録されている。

【００４９】図８は、再生機器５側における処理フローを示す。図８（ａ）におけるステップ３４１～ステップ３４４は、図６におけるステップ１０６～ステップ１０９に対応する。図８および図４を参照しながら次に再生機器５の動作フローを説明する。

【００５０】図８（ａ）において、再生機器５はまず復号鍵要求の処理を開始する（ステップ３４０）。通信手段２６は復号鍵７の発行要求をパソコン３側に送信する（ステップ３４１）。パソコン３側から再生機器５の機器ＩＤの送信が要求されると、復号鍵取得手段２８は機器ＩＤ保持手段３１に保持されている機器ＩＤを通信手段２６を介してパソコン３側に送信する（ステップ３４２）。パソコン３から復号鍵が発行されると、通信手段２６は発行された復号鍵７を受信し（ステップ３４３）、復号鍵取得手段２８は取得した復号鍵７を復号鍵保持手段２７に登録し（ステップ３４４）、処理を終了する（ステップ３４５）。

【００５１】図８（ｂ）は、再生機器５においてコンテンツを再生する際の動作フロー図である。

【００５２】まず、再生機器５はユーザの操作によりコンテンツ再生処理を開始する（ステップ３５０）。復号鍵取得手段２８は復号鍵保持手段２７が復号鍵７を所持しているかどうかを確認する（ステップ３５１）。復号鍵保持手段２７に復号鍵７が存在しない場合は、復号鍵７を取得するかどうかのステップに進む（ステップ３５２）。このステップ３５２において、復号鍵７を取得しない場合は処理を終了し（ステップ３６１）、復号鍵７を取得する場合は、図８（ａ）に示す復号鍵要求フローに進む（ステップ３５３）。復号鍵保持手段２７に復号鍵７が存在する場合は、復号鍵７に含まれる機器ＩＤと再生機器５の機器ＩＤとを比較する（ステップ３５４）。すなわち機器ＩＤ抽出手段３０は、復号鍵取得手段２８に存在する復号鍵７から機器ＩＤを抽出し、機器ＩＤ比較手段３３に渡す。また、機器ＩＤ取得手段３２は、機器ＩＤ保持手段３１に存在する固有の機器ＩＤを取得し機器ＩＤ比較手段３３に渡す。そして機器ＩＤ比較手段３３は、機器ＩＤ抽出手段３０から渡された機器ＩＤと機器ＩＤ取得手段３２から渡された機器ＩＤとが一致するかどうかを比較する（ステップ３５５）。もし、両者の機器ＩＤが一致しない場合は処理を終了する（ステップ３６１）。

【００５３】両者の機器ＩＤが一致する場合は、暗号用ＩＤ抽出手段２５は、メディアドライブ２４からコンテンツに含まれる暗号用ＩＤを取得して（ステップ３５６）、暗号・復号用ＩＤ比較手段２９に渡す。一方、復号用ＩＤ抽出手段３７は復号鍵取得手段２８に存在する復号鍵７から復号用ＩＤを抽出して暗号・復号用ＩＤ比較手段２９に渡す。そして暗号・復号用ＩＤ比較手段２９は、暗号化されたコンテンツから取得した暗号用ＩＤと復号鍵７に含まれる復号用ＩＤとを比較する（ステップ３５７）。すなわち、暗号・復号用ＩＤ比較手段２９は、暗号用ＩＤと復号用ＩＤとを比較し、両者が同じホストＩＤに対応するものであるかどうかを検証する（ステップ３５８）。

【００５４】上記の暗号用ＩＤと復号用ＩＤとが対応しない場合は再生可否判定手段３４は再生不可である判定をして処理を終了する（ステップ３６１）。両者のＩＤが対応するものである場合は、再生可否判定手段３４は再生が可能である判定を出し、復号処理手段３５は、暗号化されたコンテンツ６を復号鍵７を利用して復号化し（ステップ３５９）、出力手段３６は復号化されたコンテンツを出力することによりユーザが所望するコンテンツを再生し（ステップ３６０）、処理を終了する（ステップ３６１）。

【００５５】図９は、再生許可された再生機器５が複数台ある場合の、本発明の著作権管理システムの全体を示す模式図である。図９に示す例においては、再生機器５のうち、ポータブルＣＤプレーヤである機器Ａと、ミニコンポである機器Ｂの２台が再生許可を受けている場合を示している。このような場合、パソコン３は機器Ａに復号用ＩＤとしてＤＥＣ００１と、機器ＩＤとしてＩＤ００Ａとを有する復号鍵７を生成し、機器Ｂに復号用ＩＤとしてＤＥＣ００１と機器ＩＤとして００Ｂとを有する復号鍵７を生成する。そしてこれらの復号鍵７はそれぞれ機器Ａおよび機器Ｂに送信されている。

【００５６】ここで、暗号化されたコンテンツ６を、機器Ａで再生するため、および機器Ｂで再生するためにＣＤ－Ｒ４は、パソコン３において２枚コピーされる。このときそれぞれのＣＤ－Ｒ４には、同一の暗号化されたコンテンツ６が記録されている。すなわち、暗号化されたコンテンツ６には、同一の暗号化されたコンテンツデータとともに暗号用鍵としてＥＮＣ００１が格納されている。

【００５７】機器Ａ、および機器Ｂは、それぞれが有している復号鍵７で暗号化されたコンテンツ６を復号化して所望のコンテンツを再生する。

【００５８】図１０は、以上までの構成、動作による本

発明の著作権管理システムにより、著作権が保護されるバリエーションを図示する。

【００５９】図１０においては、ホスト装置として、パソコン３とは異なる別のパソコン４３が存在する場合を示している。また、再生機器５として機器Ａ、機器Ｂ、機器Ｃの三台が存在し、このうち機器Ａがパソコン３により復号鍵７が発行された再生機器５である状態を示している。

【００６０】上記のような条件において、まず、第三者のパソコンであるパソコン４３でコンテンツが記録されたＣＤ－Ｒを不正入手した場合を考える。この場合、パソコン４３はパソコン４３に挿入されたＣＤ－Ｒ４にパソコン４３のホストＩＤであるＩＤ００２を利用してコンテンツを暗号化し、暗号化されたコンテンツ４６には暗号鍵としてＥＮＣ００２が含まれている。ユーザが機器Ａを使用して所望のコンテンツを再生しようとすると、ＣＤ－Ｒ４が暗号化されたコンテンツ４６を有している場合、すなわち、暗号化されたコンテンツ４６にＥＮＣ００２が存在する場合、機器Ａは、上述のように、機器Ａが有する復号鍵７に含まれる復号用ＩＤであるＤＥＣ００１と、暗号化されたコンテンツ４６に含まれるＥＮＣ００２とを比較し、両者は同一のホストＩＤに由来しないことを確認する。従って機器Ａは、このようにパソコン４３で記録されたＣＤ－Ｒを不正に入手することによって得たコンテンツを再生することができない。

【００６１】次に、機器Ｂには復号鍵７が発行されていないとすると、機器Ｂは、当然ながらパソコン３によりコピーされたコンテンツもパソコン４３によりコピーされたコンテンツも再生することができない。

【００６２】次に、機器Ｃは、正規の復号鍵７を有しておらず、機器Ａの復号鍵７を不正にコピーしたものを有しているとする。その場合、機器Ｃが有する固有の機器ＩＤはＩＤ００Ｃであり、一方で不正コピーされた復号鍵７に存在する機器ＩＤは、ＩＤ００Ａであるので、機器Ｃは、両者の機器ＩＤが一致しないと判断する。従って、復号鍵７を不正コピーした機器Ｃでは、所望のコンテンツを再生することはできない。もちろん、パソコン４３により不正コピーしたコンテンツを再生することもできない。

【００６３】図１１は、以上のように場合において、著作権が保護される範囲を一覧にした図である。すなわち、再生機器５が再生許可された正規の復号鍵７を有する機器であり、ＣＤ－Ｒ４がユーザの正規のパソコン３によりコピーされた場合にのみ、ユーザが所望するコンテンツを再生することができる。しかし、再生機器５が復号鍵７を有さない機器である場合、および再生機器５が復号鍵７を不正コピーしている機器である場合は、そのようなコンテンツを再生することができない。

【００６４】図１２は、再生機器５の再生許可台数を変更しないで再生許可された再生機器５を変更するときのフローを示す図である。

【００６５】例えば、ユーザが三台の再生機器５、すなわち機器Ａ、機器Ｂ、機器Ｃを有しており、このうち機器Ａおよび機器Ｂの二台に再生許可がなされているものとする。そして、ユーザは二台という再生許可台数は変更しないで、再生許可機器を、機器Ａおよび機器Ｂから、機器Ｂおよび機器Ｃに変更する場合を例としてその場合の本実施の形態の著作権管理システムの動作を以下に説明する。

【００６６】図１２において、ステップ４０１は図６に示すステップ１０１～ステップ１０４に対応する。また、ステップ４０２は図６に示す１０５に対応し、ステップ４０３～ステップ４０６は図６に示すステップ１０６～ステップ１０９に対応する。また、ステップ４０７～ステップ４１０は、ステップ４０３～ステップ４０６に対応する動作がパソコン３と機器Ｂとの間でなされたものである。ここまで動作がさなれている状態で、機器Ａ、および機器Ｂは、ユーザが所望するコンテンツを再生することができる（ステップ４１１、ステップ４１２）。しかし、復号鍵７を有していない機器Ｃは、コンテンツを再生することができない（ステップ４１３）。

【００６７】次に、パソコン３は機器Ａに、機器Ａが有する復号鍵７を送信するよう送信要求を出す（ステップ４１４）。そして、機器Ａは、パソコン３から復号鍵７の送信要求を受けると、パソコン３に機器Ａが有する復号鍵７を送信し、機器Ａから復号鍵７を削除する（ステップ４１５）。また、パソコン３においても受け取った機器Ａの復号鍵７を復号鍵削除手段２１により削除する（ステップ２２４（図７（ｂ）参照））。

【００６８】そして、機器Ｃとパソコン３との間では、ステップ４１６～ステップ４１９において、ステップ４０３～ステップ４０６と同様の処理により、復号鍵７が機器Ｃに送信される。その結果、機器Ａでは所望のコンテンツを再生することができず（ステップ４２０）、機器Ｂおよび機器Ｃにおいて所望のコンテンツを再生することができる（ステップ４２１、４２２）。

【００６９】以上のように、本実施の形態の携帯の著作権管理システムによれば、所望のコンテンツを汎用のＣＤ－Ｒ４に複数枚コピーが可能であるので、ポータブルプレーヤ、ミニコンポ、カーステレオ等、複数の再生機器５で再生する場合、それぞれの再生機器５にセットしておくことができ、いちいちＣＤ－Ｒ４を持ち運ぶ手間をかけなくてもよい。

【００７０】本実施の形態の著作権管理システムによれば、ＣＤ－Ｒ４の複製を制限するものではなく、再生される再生機器５の台数を制限することにより、著作権の保護を図りつつもユーザの利便性を向上させることができる。

【００７１】また、ＥＭＤサーバ１は、個別の再生機器５のライセンス管理を行う必要がなく、再生機器５の使

用許可台数のみを管理すればよいので、ＥＭＤサーバ１側にとっても簡単なシステム構成で済む。

【００７２】また、所望のコンテンツを復号するための復号鍵７は、ユーザ側のパソコン３において発行されるので、ユーザはいちいちＥＭＤサーバ１側に問い合わせる必要がなく、簡単な処理で所望のコンテンツを楽しむことができる。

【００７３】なお、以上までの説明は、本発明の著作権管理システムに関するものであるが、上記の構成のシステムを利用した著作権管理方法も本発明の範囲である。

【００７４】また、以上までの説明において、ステップ１０１におけるＥＭＤサーバ１からパソコン３への台数情報３８の配信は、インターネット回線２を介してなされるとしたが、例えば郵便等のほかの方法で送信または送付されてもよい。

【００７５】また、以上までの説明では、パソコン３と再生機器５は通信ケーブルで接続されて復号鍵７のやりとり等がなされるとしたが、パソコン３と再生機器５は有線ではなく無線で接続される構成であってもよい。さらには、ＣＤ－Ｒ等の物理的なメディアを利用して復号鍵７のやりとり等がなされる構成であってもよい。その場合は、パソコン３と再生機器５との間の復号鍵７等のやりとりは送信または受信ではなく、送られ、または受け取られる動作となる。そのような場合も上記と同様の効果を得ることができる。

【００７６】また、以上までの説明では、暗号化されたコンテンツが記録されるメディアは、ＣＤ－Ｒであるとしたが、他のメディアであっても当然よい。

【００７７】また、以上までの説明では、パソコン３は、再生許可された台数以内の再生機器５に復号鍵７を発行するとしたが、さらに特定の機器に復号鍵７の発行を制限する機能があってもよい。そのような例として、例えば、高音質対応の再生機器５にのみ復号鍵７を発行する構成であってもよい。

【００７８】また、以上までの説明におけるコンテンツには、音楽データのみならず、静止画像データ、動画データ、文字データ、その他の情報も含まれる。すなわち、本発明の配信サーバは、ＥＭＤサーバ１に限定されず、上記のようなさまざまのコンテンツを配信することができるサーバであってもよい。

【００７９】また、以上までの説明では、本発明のホスト装置は、パソコン３、４３であるとしたが、本発明のホスト装置は上記の機能を果たすことができればパソコン以外の機器であってもよい。そのような例としては例えば携帯電話、携帯端末等が挙げられるがこれらに限定されない。

【００８０】また、以上までの説明では、再生機器５は一台または三台である例を説明したが、再生機器５が再生許可台数以内であれば何台であってもよいことは言うまでもない。また、再生許可台数を変更したい場合は、図６に示すステップ１０１において再生許可台数の変更を配信サーバ側に通知すればよい。

【００８１】また、本発明のプログラムは、上述した本発明の著作権管理システムの全部又は一部の手段（又は、装置、素子等）の機能をコンピュータにより実行させるためのプログラムであって、コンピュータと協働して動作するプログラムである。

【００８２】又、本発明の記録媒体は、上述した本発明の著作権管理システムの全部又は一部の手段（又は、装置、素子等）の全部又は一部の機能をコンピュータにより実行させるためのプログラムを担持した記録媒体であり、コンピュータにより読み取り可能且つ、読み取られた前記プログラムが前記コンピュータと協動して前記機能を実行する記録媒体である。

【００８３】尚、本発明の上記「一部の手段（又は、装置、素子等）」とは、それらの複数の手段の内の、一つ又は幾つかの手段を意味し、本発明の上記「一部のステップ（又は、工程、動作、作用等）」とは、それらの複数のステップの内の、一つ又は幾つかのステップを意味する。

【００８４】又、本発明の上記「手段（又は、装置、素子等）の機能」とは、前記手段の全部又は一部の機能を意味し、本発明の上記「ステップ（又は、工程、動作、作用等）の動作」とは、前記ステップの全部又は一部の動作を意味する。

【００８５】又、本発明のプログラムの一利用形態は、コンピュータにより読み取り可能な記録媒体に記録され、コンピュータと協働して動作する態様であっても良い。

【００８６】又、本発明のプログラムの一利用形態は、伝送媒体中を伝送し、コンピュータにより読みとられ、コンピュータと協働して動作する態様であっても良い。

【００８７】又、本発明のデータ構造としては、データベース、データフォーマット、データテーブル、データリスト、データの種類などを含む。

【００８８】又、記録媒体としては、ＲＯＭ等が含まれ、伝送媒体としては、インターネット等の伝送媒体、光・電波・音波等が含まれる。

【００８９】又、上述した本発明のコンピュータは、ＣＰＵ等の純然たるハードウェアに限らず、ファームウェアや、ＯＳ、更に周辺機器を含むものであっても良い。

【００９０】尚、以上説明した様に、本発明の構成は、ソフトウェア的に実現しても良いし、ハードウェア的に実現しても良い。

【００９１】

【発明の効果】本発明によれば、ユーザにとって使い勝手がよい著作権保護システム、著作権保護方法、そのホスト装置、そのプログラム、そのプログラムを担持した記録媒体を提供することができる。

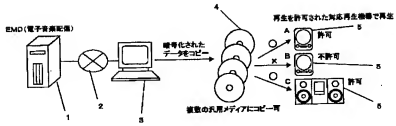
【図面の簡単な説明】

【図１】図１は、本発明の実施の形態の著作権管理システムの概要を示す図である。
【図２】図２は、本発明の実施の形態の著作権管理システムの動作の概要を示す図である。
【図３】図３は、本発明の実施の形態の著作権管理システムを構成するパソコンの構成を示すブロック図である。
【図４】図４は、本発明の実施の形態の著作権管理システムを構成する再生機器の構成を示すブロック図である。
【図５】図５は、本発明の実施の形態の著作権管理システムの全体の動作を示す概略図である。
【図６】図６は、本発明の実施の形態の著作権管理システムの全体の動作を示すフロー図である。
【図７】図７は、本発明の実施の形態の著作権管理システムを構成するパソコンの動作を示すフロー図である。
【図８】図８は、本発明の実施の形態の著作権管理システムを構成する再生機器の動作を示すフロー図である。
【図９】図９は、本発明の実施の形態の著作権管理システムの全体の動作を示す概略図である。
【図１０】図１０は、本発明の実施の形態の著作権管理システムにより保護される著作権のバリエーションを示す図である。
【図１１】図１１は、本発明の実施の形態の著作権管理システムにより保護される著作権のバリエーションを示す図である。
【図１２】図１２は、本発明の実施の形態の著作権管理システムを構成する再生機器の再生許可台数変更する際の動作を示すフロー図である。
【図１３】図１３は、従来技術の著作権管理システムの概略図である。
【図１４】図１４は、従来技術の著作権管理システムの概略図である。
【符号の説明】
１　　ＥＭＤサーバ
２　　インターネット回線
３、４３　パソコン
４　　ＣＤ－Ｒ
５　　再生機器
６　　暗号化されたコンテンツ
７　　復号鍵
８　　復号手段
９　　コンテンツ暗号化手段
１０　記録手段
１１　鍵入手手段
１２　鍵管理情報データベース
１３　鍵管理情報制御手段
１４　自ＩＤ保持手段
１５　自ＩＤ取得手段
１６　暗号用ＩＤ復号用ＩＤ生成手段
１７　復号鍵生成手段
１８　復号鍵発行手段
１９、２２、２６　通信手段
２０　機器ＩＤ入手手段
２１　復号鍵削除手段
２３　コンテンツ入手手段
２４　メディアドライブ
２５　暗号用ＩＤ抽出手段
２７　復号鍵保持手段
２８　復号鍵取得手段
２９　暗号符号用ＩＤ比較手段
３０　機器ＩＤ抽出手段
３１　機器ＩＤ保持手段
３２　機器ＩＤ取得手段
３３　機器ＩＤ比較手段
３４　再生可否判定手段
３５　復号処理手段３６　出力手段
３７　復号用ＩＤ抽出手段
３８　鍵

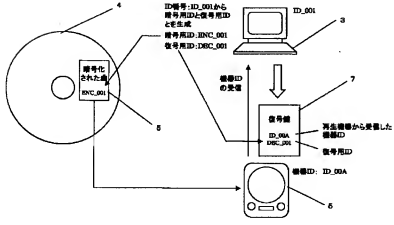
【図１１】

再生機器	暗号機器	暗号データ中の暗号用ID	復号鍵中の暗号用ID	再生機器の機器ID	復号鍵中の機器ID	再生の可否	備考
機器A	PC1	ENC_001	DEC_001	ID_00A	ID_00A	○	正常の再生
機器A	PC2	ENC_002	DEC_001	ID_00A	ID_00A	×	余当のPCで暗号化されたデータを不正入手した場合
機器B	PC1	ENC_001	---	ID_00B	---	×	再生機器に復号鍵がない場合
機器B	PC2	ENC_002	---	ID_00B	---	×	再生機器に復号鍵がない場合
機器C	PC1	ENC_001	DEC_001	ID_00C	ID_00A	×	復号鍵を不正入手した場合
機器C	PC2	ENC_002	DEC_001	ID_00C	ID_00A	×	復号鍵を不正入手した場合

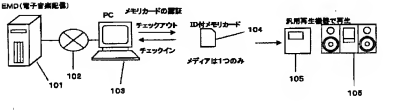
【図１】


EMD(電子音楽配信)
暗号化された
データをコピー
再生を許可された再生機器で再生
A
許可
K
B
不許可
C
許可
被登の汎用メディアにコピー可
1
2
3
4
5
6

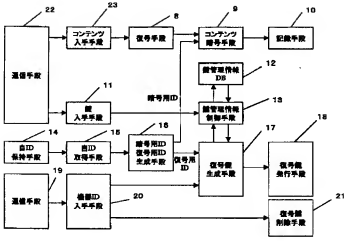
【図２】


ID番号:ID_001から
暗号用IDと復号用ID
とを生成
暗号用ID:ENC_001
復号用ID:DEC_001
ID_001
暗号化
された曲
ENC_001
機器ID
の受信
復号鍵
ID_00A
DEC_001
再生機器から受信した
機器ID
復号用ID
機器ID: ID_00A
3
4
5
6
7

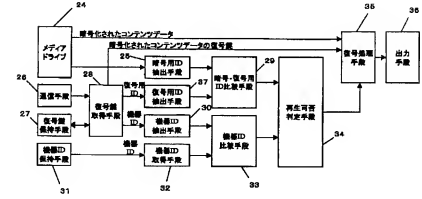
【図１３】


EMD(電子音楽配信)
PC
メモリカードの認証
チェックアウト
チェックイン
ID付メモリカード
104
メディアは1つのみ
汎用再生機器で再生
101
102
103
105
106

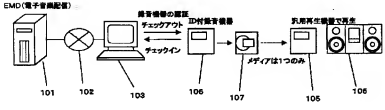
【図３】


通信手段
コンテンツ入手手段
復号手段
コンテンツ暗号手段
記録手段
著管理情報DB
鍵入手手段
暗号用ID
著管理情報制御手段
自ID保持手段
自ID取得手段
暗号用ID復号用ID生成手段
復号用ID
復号鍵生成手段
復号鍵格納手段
通信手段
機器ID入手手段
復号鍵削除手段

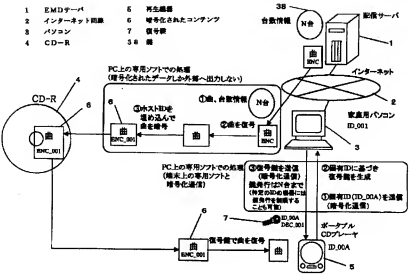
【図４】


メディアドライブ
暗号化されたコンテンツデータ
復号化されたコンテンツデータの復号鍵
通信手段
復号鍵保持手段
機器ID保持手段
復号鍵取得手段
暗号用ID抽出手段
復号用ID抽出手段
機器ID抽出手段
機器ID取得手段
暗号・復号用ID比較手段
機器ID比較手段
再生可否判定手段
復号処理手段
出力手段

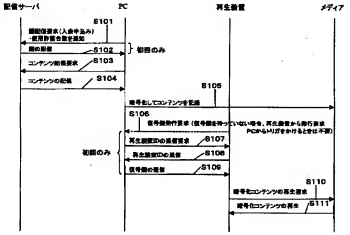
【図１４】


EMD(電子著鍵配信)
著者機器の認証
チェックアウト
チェックイン
ID付著者機器
メディアは１つのみ
汎用再生機器で再生

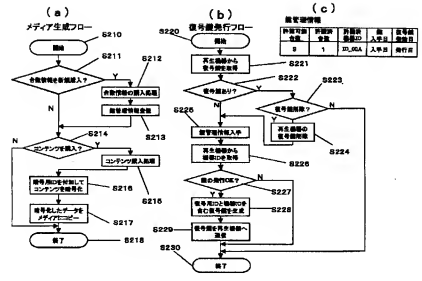
【図５】


1　EMDサーバ
2　インターネット回線
3　パソコン
4　CD−R
5　再生機器
6　暗号化されたコンテンツ
7　復号鍵
38　鍵
台数情報
N台
配信サーバ
曲
ENC
インターネット
PC上の専用ソフトでの処理
（暗号化されたデータしか外部へ出力しない）
CD-R
①曲、台数情報
③ホストIDを埋め込んで曲を暗号
②曲を復号
ENC_001
家庭用パソコン
ID_001
PC上の専用ソフトでの処理
（端末上の専用ソフトと暗号化通信）
③復号鍵を送信
（暗号化通信）
鍵発行はN台まで
（特定のIDの機器には鍵発行を制限することも可能）
②固有IDに基づき復号鍵を生成
①固有ID（ID_00A）を送信
（暗号化通信）
ID_00A
DEC_001
ポータブルCDプレーヤ
復号鍵で曲を復号

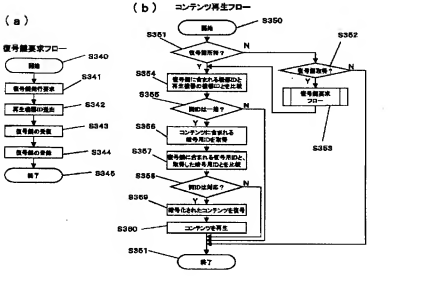
【図６】


配信サーバ
PC
再生装置
メディア
S101
鍵配信要求（入会申込み）
・使用許諾台数を通知
鍵の配信
S102
初回のみ
コンテンツ配信要求
S103
コンテンツの配信
S104
S105
暗号化してコンテンツを記録
S106
復号鍵発行要求（復号鍵を持っていない場合、再生装置から発行要求
PCからトリガをかけるときは不要）
再生装置IDの送信要求
S107
初回のみ
再生装置IDの送信
S108
復号鍵の送信
S109
S110
暗号化コンテンツの再生要求
暗号化コンテンツの再生
S111

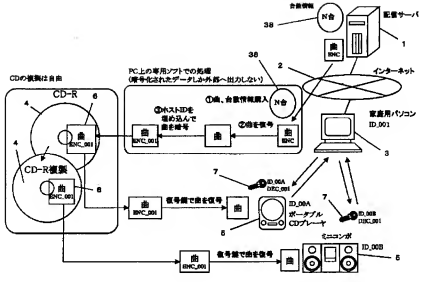
【図７】


（ａ）
メディア生成フロー
開始
S210
S211
S212
S213
S214
S215
S216
S217
S218
（ｂ）
復号鍵発行フロー
S220
開始
S221
S222
S223
S224
S225
S226
S227
S228
S229
S230
（ｃ）
鍵管理情報
許容可能
台数
許諾
台数
許諾鍵
識別ID
鍵
入手日
鍵有
効期日
3
1
ID_KKA
入手日
発行日

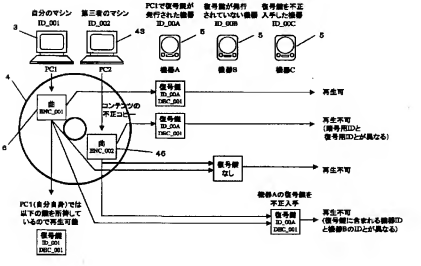
【図８】


（ａ）
復号鍵要求フロー
開始
S340
S341
S342
S343
S344
S345
（ｂ）
コンテンツ再生フロー
開始
S350
S351
S352
S353
S354
S355
S356
S357
S358
S359
S360
S361

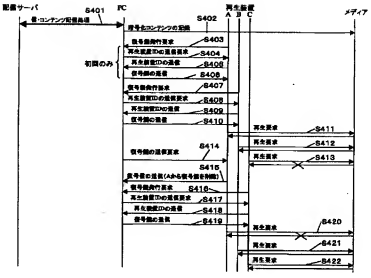
【図９】


CDの状態は自由
CD-R
CD-R複製
PC上の専用ソフトでの処理
(暗号化されたデータしか外部へ出力しない)
①曲、会員情報購入
②ホストIDを
埋め込んで
曲を暗号
②曲を暗号
暗号鍵で曲を復号
暗号鍵で曲を復号
暗号鍵で曲を復号
N会
配信サーバ
インターネット
家庭用パソコン
ID_001
ID_00A
ポータブル
CDプレーヤ
ID_00B
ミニコンポ
曲
BMC_001
BMC_00A
BMC_00B

【図１０】


自分のマシン
ID_001
第三者のマシン
ID_002
PC1で復号鍵が
発行された機器
ID_00A
復号鍵が発行
されていない機器
ID_00B
復号鍵を不正
入手した機器
ID_00C
PC1
PC2
機器A
機器B
機器C
曲
BMC_001
コンテンツの
再圧コード
曲
BMC_002
復号鍵
ID_00A
BMC_001
復号鍵
ID_00A
BMC_001
復号鍵
なし
再生可
再生不可
(復号用IDと
復号用IDとが異なる)
再生不可
PC1(自分自身)では
以下の曲を所有して
いるので再生可能
復号鍵
ID_001
BMC_001
機器Aの復号鍵を
不正入手
復号鍵
ID_00A
BMC_001
再生不可
(復号鍵に含まれる機器ID
と機器BのIDとが異なる)

【図１２】



フロントページの続き

(51)Int.Cl.7	識別記号	F I	ﾃｰﾏｺｰﾄﾞ（参考）
Ｈ０４Ｌ 9/08		Ｈ０４Ｌ 9/00	６０１Ｄ
9/32			６０１Ｅ
			６７３Ｂ

Ｆターム(参考) 5B017 AA06 BB10 CA16
5D044 AB05 BC05 DE50 GK12 GK17
HL08 HL11
5D110 AA16 AA27 BB01 BB25 BB29
DA08
5J104 AA12 AA16 EA01 EA04 EA18
JA03 KA02 KA15 MA05 NA02
PA07 PA14